Please replace the paragraph beginning at page 56, line 21, with the following rewritten paragraph:

A39

--When this copyright management apparatus 140 is used, no decrypted data is present outside the copyright management apparatus 140.--

IN THE CLAIMS:

Please amend the claims, as follows:

A37

1. (Amended) A method for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from encrypted digital data, said method comprising the steps of:

encrypting said decrypted digital data using a changeable key to produce changeable key re-encrypted digital data;

encrypting said changeable key re-encrypted digital data using an unchangeable key in a device to produce changeable-unchangeable keys double re-encrypted digital data to be stored, copied or transferred;

decrypting said copied, stored or transferred changeable-unchangeable keys double re-encrypted digital data using said unchangeable key to said changeable key re-encrypted digital data; and

decrypting said changeable key re-encrypted digital data using said changeable key to said decrypted digital data.

#37

2. (Amended) A method for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from encrypted digital data, comprising the steps of:

encrypting said decrypted digital data using an unchangeable key in a device to produce unchangeable key re-encrypted digital data;

encrypting said unchangeable key re-encrypted digital data using a changeable key to produce unchangeable-changeable keys double re-encrypted digital data to be stored, copied or transferred;

decrypting said copied, stored or transferred unchangeable-changeable keys double re-encrypted digital data using said changeable key to said unchangeable key re-encrypted digital data; and

decrypting said unchangeable key re-encrypted digital data using said unchangeable key to said decrypted digital data.

3. (Amended) The method according to claim 1 or 2, wherein said steps of encrypting and decrypting using said changeable key are carried out by a software.

4. (Amended) The method according to claim 1 or 2, wherein said steps of encrypting and decrypting using said changeable key are carried out by a hardware.

5. (Amended) The method according to claim 1 or 2, wherein said changeable key is supplied externally from said device.

6. (Amended) The method according to claim 1 or 2, wherein said changeable key is generated in said device.

7. (Amended) The method according to claim 1 or 2, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a software.

8. (Amended) The method according to claim 1 or 2, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a hardware.

9. (Amended) The method according to claim 1 or 2, wherein said unchangeable key is already placed in said device.

10. (Amended) The method according to claim 1 or 2, wherein said unchangeable key is generated in said device.

11. (Amended) The method according to claim 1 or 2, wherein said unchangeable key is supplied externally from said device.

#37

12. (Amended) The method according to claim 9, 10 or 11, wherein said unchangeable key is specific to said device.

13. (Amended) The method according to claim 9, 10 or 11, wherein said unchangeable key is not specific to said device.

14. (Amended) An apparatus for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from encrypted digital data, said apparatus comprising:

a changeable key encryption unit for encrypting said decrypted digital data using a changeable key to produce changeable key re-encrypted digital data;

an unchangeable key encryption unit for encrypting said changeable key re-encrypted digital data using an unchangeable key in a device to produce changeable-unchangeable keys double re-encrypted digital data to be stored, copied or transferred;

an unchangeable key decryption unit for decrypting said copied, stored or transferred changeable-unchangeable keys double re-encrypted digital data using said unchangeable key to said changeable key re-encrypted digital data; and

a changeable key decryption unit for decrypting said changeable key re-encrypted digital data using said changeable key to said decrypted digital data.

15. (Amended) An apparatus for protecting decrypted digital data, from illegitimate use, said decrypted digital data being decrypted from encrypted digital data, said apparatus comprising:

an unchangeable key encryption unit for encrypting said decrypted digital data using an unchangeable key in a device to produce unchangeable key re-encrypted digital data;

a changeable key encryption unit for encrypting said unchangeable key re-encrypted digital data using a changeable key to produce changeable-unchangeable keys double re-encrypted digital data to be stored, copied or transferred;

a changeable key decryption unit for decrypting said copied, stored or transferred changeable-unchangeable keys double re-encrypted digital data using said changeable key to said unchangeable key re-encrypted digital data; and

an unchangeable key decryption unit for decrypting said unchangeable key re-encrypted digital data using said unchangeable key to said decrypted digital data.

16. (Amended) The apparatus according to claim 14 or 15, in which encrypting and decrypting using said changeable key are carried out by a software.

17. (Amended) The apparatus according to claim 14 or 15, in which encrypting and decrypting using said changeable key are carried out by a hardware.

A37

18. (Amended) The apparatus according to claim 14 or 15, wherein said changeable key is supplied externally from said device.

19. (Amended) The apparatus according to claim 14 or 15, wherein said changeable key is generated in said device.

20. (Amended) The apparatus according to claim 14 or 15, in which encrypting and decrypting using said unchangeable key are carried out by a software.

21. (Amended) The apparatus according to claim 14 or 15, in which encrypting and decrypting using said unchangeable key are carried out by a hardware.

22. (Amended) The apparatus according to claim 14 or 15, wherein said unchangeable key is already placed in said device.

23. (Amended) The apparatus according to claim 14 or 15, wherein said unchangeable key is generated in said device.

24. (Amended) The apparatus according to claim 14 or 15, wherein said unchangeable key is supplied externally from said device.

37

25. (Amended) The apparatus according to claim 14 or 15, wherein said unchangeable key is specific to said device.

26. (Amended) The apparatus according to claim 14 or 15, wherein said unchangeable key is not specific to said device.

27. (Amended) A method for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said method comprising the steps of:

encrypting said decrypted digital data using a second changeable key to produce second changeable key re-encrypted digital data;

encrypting said second changeable key re-encrypted digital data using an unchangeable key in a device to produce unchangeable-second changeable keys double re-encrypted digital data to be stored;

decrypting said stored unchangeable-second changeable keys double re-encrypted digital data using said unchangeable key to said second changeable key re-encrypted digital data;

encrypting said second changeable key re-encrypted digital data using a third changeable key to produce third changeable-second changeable keys double re-encrypted digital data to be copied or transferred;

decrypting said copied or transferred third changeable-second changeable keys double re-encrypted digital data double using said third changeable key to said second changeable key re-encrypted digital data; and

decrypting said second changeable key re-encrypted digital data using said second changeable key to said decrypted digital data.

28. (Amended) A method for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said method comprising the steps of:

encrypting said decrypted digital data using a second changeable key to produce second changeable key re-encrypted digital data;

encrypting said second changeable key re-encrypted digital data using an unchangeable key in a device to produce unchangeable-second changeable keys double re-encrypted digital data to be stored;

decrypting said stored unchangeable-second changeable keys double re-encrypted digital data double using said unchangeable key to said second changeable key re-encrypted digital data;

encrypting said second changeable key re-encrypted digital data using a third changeable key to produce third changeable-second changeable keys double re-encrypted digital data to be copied or transferred;

decrypting said copied or transferred third changeable-second changeable keys double re-encrypted digital data double using said third changeable key to said second changeable key re-encrypted digital data; and

decrypting said second changeable key re-encrypted digital data using said second changeable key to said decrypted digital data.

29. (Amended) A method for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said method comprising the steps of:

encrypting said decrypted digital data using an unchangeable key in a device to produce unchangeable key re-encrypted digital data, and encrypting said unchangeable key re-encrypted digital data using a second changeable key to produce second changeable-unchangeable keys double re-encrypted digital data double to be stored;

decrypting said stored second changeable-unchangeable keys double re-encrypted digital data double using said second changeable key to said unchangeable key re-encrypted digital data;

decrypting said unchangeable key re-encrypted digital data using said unchangeable key to said decrypted digital data;

encrypting said decrypted digital data using a third changeable key to produce third changeable key re-encrypted digital data, and encrypting said third changeable key re-encrypted digital data using said second changeable key to produce second changeable-third changeable keys double re-encrypted digital data to be copied or transferred;

decrypting said copied or transferred second changeable-third changeable keys double re-encrypted digital data using said second changeable key to said third changeable key re-encrypted digital data; and

decrypting said third changeable key re-encrypted digital data using said third changeable key to said decrypted digital data.

30. (Amended) A method for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said method comprising the steps of:

encrypting said decrypted digital data using an unchangeable key in a device to produce unchangeable key re-encrypted digital data, and encrypting said unchangeable key re-encrypted digital data using a second changeable key to produce second changeable-unchangeable keys double re-encrypted digital data;

decrypting said stored second changeable-unchangeable keys double re-encrypted digital data using said second changeable key to said unchangeable key re-encrypted digital data;

decrypting said unchangeable key re-encrypted digital data using said unchangeable key to said decrypted digital data;

encrypting said decrypted digital data using a third changeable key to produce third changeable key re-encrypted digital data, and encrypting said third changeable key re-encrypted digital data using said second changeable key to produce second changeable-third changeable keys double re-encrypted digital data to be copied or transferred;

decrypting said copied or transferred second changeable-third changeable keys double re-encrypted digital data using said second changeable key to said third changeable key re-encrypted digital data; and

decrypting said third changeable key re-encrypted digital data using said third changeable key to said decrypted digital data.

31. (Amended) The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting using said second changeable key are carried out by a software.

32. (Amended) The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting using said second changeable key are carried out by a hardware.

33. (Amended) The method according to claim 27, 28, 29 or 30, wherein said second changeable key is supplied externally from said device.

34. (Amended) The method according to claim 27, 28, 29 or 30, wherein said second changeable key is generated in said device.

437

35. (Amended) The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting using said third changeable key are carried out by a software.

36. (Amended) The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting using said third changeable key are carried out by a hardware.

37. (Amended) The method according to claim 27, 28, 29 or 30, wherein said third changeable key is supplied externally from said device.

38. (Amended) The method according to claim 27, 28, 29 or 30, wherein said third changeable key is generated in said device.

39. (Amended) The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a software.

40. (Amended) The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a hardware.

41. (Amended) The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is already placed in said device.

A37

42. (Amended) The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is generated in said device.

43. (Amended) The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is supplied externally from said device.

44. (Amended) The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is specific to said device.

45. (Amended) The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is not specific to said device.

46. (Amended) An apparatus for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said apparatus comprising:

a second changeable key encryption unit for encrypting said decrypted digital data using a second changeable key to produce second changeable key re-encrypted digital data;

an unchangeable key encryption unit for encrypting said second changeable key re-encrypted digital data using an unchangeable key in a device to produce unchangeable-second changeable keys double re-encrypted digital data to be stored;

an unchangeable key decryption unit for decrypting said stored unchangeable-second changeable keys double re-encrypted digital data using said unchangeable key to said second changeable key re-encrypted digital data;

a third changeable key encryption unit for encrypting said second changeable key re-encrypted digital data using a third changeable key to produce third changeable-second changeable keys double re-encrypted digital data to be copied or transferred;

a third changeable key decryption unit for decrypting said copied or transferred third changeable-second changeable keys double re-encrypted digital data using said third changeable key to said second changeable key re-encrypted digital data; and

a second changeable key decryption unit for decrypting said second changeable key re-encrypted digital data using said second changeable key to said decrypted digital data.

47. (Amended) An apparatus for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said apparatus comprising:

a second changeable key encryption unit for encrypting said decrypted digital data using a second changeable key to produce second changeable key re-encrypted digital data;

an unchangeable key encryption unit for encrypting said second changeable key re-encrypted digital data using an unchangeable key in a device to produce unchangeable-second changeable keys double re-encrypted digital data to be stored;

an unchangeable key decryption unit for decrypting said stored unchangeable-second changeable keys double re-encrypted digital data using said unchangeable key to said second changeable key re-encrypted digital data;

a third changeable key encryption unit for encrypting said second changeable key re-encrypted digital data using a third changeable key to produce third changeable-second changeable keys double re-encrypted digital data [double re-encrypted by third-changeable-second-changeable keys] to be copied or transferred;

a third changeable key decryption unit for decrypting said copied or transferred third changeable-second changeable keys double re-encrypted digital data using said third changeable key to said second changeable key re-encrypted digital data; and

a second changeable key decryption unit for decrypting said second changeable key re-encrypted digital data using said second changeable key to said decrypted digital data.

48. (Amended) An apparatus for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said apparatus comprising:

an unchangeable key encryption unit for encrypting said decrypted digital data using an unchangeable key in a device to produce unchangeable key re-encrypted digital data, and a second changeable key encryption unit for encrypting said unchangeable key re-encrypted digital data using a second changeable key to produce second changeable-unchangeable keys double re-encrypted digital data to be stored;

a second changeable key decryption unit for decrypting said stored second changeable-unchangeable keys double re-encrypted digital data using said second changeable key to said unchangeable key re-encrypted digital data, and an unchangeable key decryption unit for decrypting said unchangeable key re-encrypted digital data using said unchangeable key to said decrypted digital data;

a third changeable key encryption unit for encrypting said decrypted digital data using a third changeable key to produce third changeable key re-encrypted digital data, and a second changeable key encryption unit for encrypting said third changeable key re-encrypted digital data using said second changeable key to produce second changeable-third changeable keys double re-encrypted digital data to be copied or transferred; and

a second changeable key decryption unit for decrypting said copied or transferred second changeable-third changeable keys double re-encrypted digital data using said second changeable key to said third changeable key re-encrypted digital data, and a third changeable key decryption unit for decrypting said third changeable key re-encrypted digital data using said third changeable key to said decrypted digital data.

49. (Amended) An apparatus for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said apparatus comprising:

an unchangeable key encryption unit for encrypting said decrypted digital data using an unchangeable key in a device to produce unchangeable key re-encrypted digital data, and a second changeable key encryption unit for encrypting said unchangeable key re-encrypted digital data using a second changeable key to produce second changeable-unchangeable keys double re-encrypted digital data to be stored;

a second changeable key decryption unit for decrypting said stored second changeable-unchangeable keys double re-encrypted digital data using said second changeable key to said unchangeable key re-encrypted digital data, and an unchangeable key decryption unit for decrypting said unchangeable key re-encrypted digital data using said unchangeable key to said decrypted digital data;

a third changeable key encryption unit for encrypting said decrypted digital data using a third changeable key to produce third changeable key re-encrypted digital data, and a second changeable key encryption unit for encrypting said third changeable key re-encrypted digital data using said second changeable key to produce second changeable-third changeable keys double re-encrypted digital data to be copied or transferred; and

a second changeable key decryption unit for decrypting said copied or transferred second changeable-third changeable keys double re-encrypted digital data using said second changeable key to said third changeable key re-encrypted digital data, and a third changeable key decryption unit for decrypting said third changeable key re-encrypted digital data using said third changeable key to said decrypted digital data.

A37

50. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting using said second changeable key are carried out by a software.

51. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting using said second changeable key are carried out by a hardware.

52. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said second changeable key is supplied externally from said device.

53. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said second changeable key is generated in said device.

54. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting using said third changeable key are carried out by a software.

55. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting using said third changeable key are carried out by a hardware.

A37

56. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said third changeable key is supplied externally from said device.

57. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said third changeable key is generated in said device.

58. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a software.

59. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a hardware.

60. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is already placed in the device.

61. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is generated in the device.

62. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is supplied externally from the device.

A37

63. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is specific to said device.

64. (Amended) The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is not specific to said device.

65. (Amended) A method for protecting digital data from illegitimate use, said method comprising the steps of:

determining whether said digital data is subject to be protected or not;

encrypting said digital data, determined to be protected, using an unchangeable key in a device to produce unchangeable key encrypted digital data;

storing, copying or transferring said unchangeable key encrypted digital data;

decrypting said stored, copied or transferred unchangeable key encrypted digital data using said unchangeable key to said decrypted digital data; and

utilizing said stored, copied or transferred unchangeable key encrypted digital data and said decrypted digital data.

66. (Amended) The method according to claim 65, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a software.

A37

67. (Amended) The method according to claim 65, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a hardware.

68. (Amended) The method according to claim 65, in which encrypting and decrypting using said unchangeable key are controlled by identifying information which is added to said digital data.

69. (Amended) The method according to claim 68, in which encrypting and decrypting are carried out when said identifying information is present.

70. (Amended) The method according to claim 68, in which encrypting and decrypting are carried out when said identifying information is absent.

71. (Amended) The method according to claim 65, wherein said unchangeable key is already placed in said device.

72. (Amended) The method according to claim 65, wherein said unchangeable key is generated in the device.

A37

73. (Amended) The method according to claim 65, wherein said unchangeable key is supplied externally from the device.

74. (Amended) The method according to claim 71, 72 or 73, wherein said unchangeable key is specific to the device.

75. (Amended) The method according to claim 71, 72 or 73, wherein said unchangeable key is not specific to the device.

76. (Amended) An apparatus for protecting digital data from illegitimate use, said apparatus comprising:

determining means for determining whether said digital data is subject to be protected or not;

means for encrypting said digital data, determined being subject to be protected, using an unchangeable key in a device to produce unchangeable key encrypted digital data;

means for storing, copying or transferring said unchangeable key encrypted digital data;

means for decrypting said stored, copied or transferred unchangeable key encrypted digital data to said decrypted digital data; and

A37

means for utilizing said stored, copied or transferred unchangeable key encrypted digital data and said decrypted digital data.

77. (Amended) The apparatus according to claim 76, wherein encrypting and decrypting using said unchangeable key are carried out by a software.

78. (Amended) The apparatus according to claim 76, wherein encrypting and decrypting using said unchangeable key are carried out by a hardware.

79. (Amended) The apparatus according to claim 76, wherein encrypting and decrypting using said unchangeable key are controlled by identifying information which is added to said digital data.

80. (Amended) The apparatus according to claim 76, wherein encrypting and decrypting are carried out when said identifying information is present.

81. (Amended) The apparatus according to claim 76, wherein encrypting and decrypting are carried out when said identifying information is absent.

A37

82. (Amended) The apparatus according to claim 76, wherein said unchangeable key is already placed in the device.

83. (Amended) The apparatus according to claim 76, wherein said unchangeable key is generated in the device.

84. (Amended) The apparatus according to claim 76, wherein said unchangeable key is supplied externally from the device.

85. (Amended) The apparatus according to claim 82, 83 or 84, wherein said unchangeable key is specific to the device.

86. (Amended) The apparatus according to claim 82, 83 or 84, wherein said unchangeable key is not specific to the device.